2018/5/17

المحاضرة الثامنة "نظرية أويلر"

دالة أويلر: هي الدالة التي تقبل

مبرهنة أويلر: $a \in \mathbb{Z}$ $N \in n$ $d(a,n)=1$ عندئذ $a^{\varphi(n)} \equiv 1 \pmod{n}$

الإثبات: $(\mathbb{Z}_n, +, \cdot)$ حلقة زمرتها الضربية تتألف

$$U(\mathbb{Z}_m) = \{\bar{a} \in \mathbb{Z}_m : d(a,m)=1\}$$

$d(a,m)=1$ من الفرض $\Leftarrow$ $\bar{a} \in U(\mathbb{Z}_m)$ ولكن من مبرهنة لاغرانج

مبرهنة لاغرانج: $|G|=m$ $x \in G : x^m = e$

ومنه نجد أن $(\bar{a})^{|U(\mathbb{Z}_n)|} = \bar{1}$ ومنه ثم $(\bar{a})^{\varphi(n)} = \bar{1}$

$\Leftarrow$ $\bar{a}^{\varphi(n)} = \bar{1}$ ومنه $a^{\varphi(n)} \equiv 1 \pmod{n}$

نتيجة: إن مبرهنة فيرما حالة خاصة من أويلر إذا كان

$P \nmid a$ فإن $a^{P-1} \equiv 1 \pmod{P}$ $\Leftarrow$ $d(p,a)=1$

وحيث أن $\varphi(P)=P-1$ ومنه من أويلر

$$a^{P-1} \equiv 1 \pmod{P}$$

مبرهنة 2: إذا كان $n=P^{\alpha}$ حيث أن P عدد أولي و α عدد صحيح

موجب فإن $\varphi(P^{\alpha}) =$

نتيجة: إذا كانت العبارة القانونية $n = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k}$ فإن

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{P_i}\right)$$

الإثبات: φ دالة ضربية وبما أن $P_1, P_2, \cdots P_k$ أعداد

أولية مختلفة فهي أولية نسبية مثنى مثنى وبالتالي فإن

$P_1^{\alpha_1}, P_2^{\alpha_2}$ أولية نسبياً مثنى مثنى

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k})$$

$$= \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)$$

$$= \underbrace{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{n}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$$n \cdot \prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

مثال $\varphi(360)$

نحلل العدد الى عوامله الأولية

360	2
180	2
90	2
45	3
15	3
5	5
1	

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$\varphi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 360\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)$$

$$= 360\,\frac{4}{15} = 96$$

أي

$$|U(\mathbb{Z}_{360})| = 96$$

$$U(\mathbb{Z}_{360}) = \{a \in \mathbb{Z} : (a, 360) = 1\}$$

بعض التمارين البسيطة

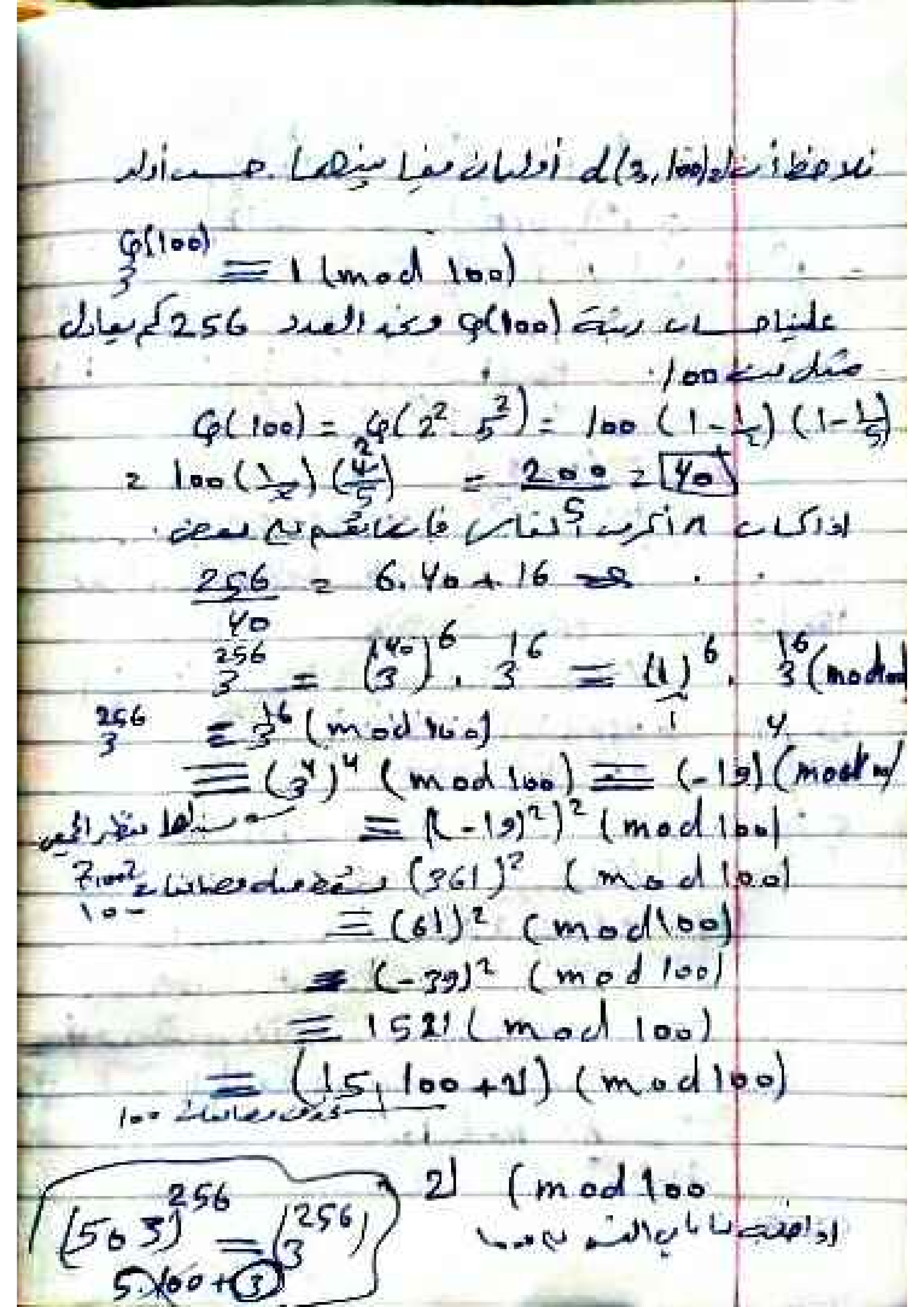
مثال

أوجد رقمي الآحاد والعشرات للعدد 3^{256}

العدد المطلوب هو باقي قسمة هذا العدد على 100

$$3^{256} \equiv x \pmod{100}$$

هو هذا العدد



نلاحظ أن $d(3,100)=1$ أي أنهما أوليان فيما بينهما. حسب أويلر

$$3^{\varphi(100)} \equiv 1 \pmod{100}$$

علينا أن نحسب $\varphi(100)$ ونجد العدد 256 كم يعادل مثلاً من 100:

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$$

$$= 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = \frac{200}{5} = \boxed{40}$$

إذا كان n أكبر فإننا نقسم على بعض:

$$\frac{256}{40} = 6 \cdot 40 + 16$$

$$3^{256} = \left(3^{40}\right)^6 \cdot 3^{16} \equiv (1)^6 \cdot 3^{16} \pmod{100}$$

$$3^{256} \equiv 3^{16} \pmod{100}$$

$$\equiv \left(3^4\right)^4 \pmod{100} \equiv (-19)^4 \pmod{100}$$

[illegible] $\equiv \left((-19)^2\right)^2 \pmod{100}$

[illegible] $\equiv (361)^2 \pmod{100}$

$$\equiv (61)^2 \pmod{100}$$

$$\equiv (-39)^2 \pmod{100}$$

$$\equiv 1521 \pmod{100}$$

$$\equiv (15 \cdot 100 + 21) \pmod{100}$$

[illegible]

$$(503)^{256} \equiv \left(3^{256}\right) \equiv 21 \pmod{100}$$

$503 = 5 \cdot 100 + 3$

إذا [illegible]

أترك لك الأسئلة أكبر عدد من المسائل المشابهة بالسابق
لـ على فهم التعامل معه مع دالة أويلر

نفرض أن $n, m \in \mathbb{Z}^+$ بحيث أن
$d(n,m)=1$ أي أوليان فيما بينهما

عندئذ اثبت أن

$$\left[m^{\varphi(n)} + n^{\varphi(m)}\right] \equiv 1 \pmod{m \cdot n}$$

من أويلر بما أن $d(n,m)=1$

$$m^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow n \mid \left[m^{\varphi(n)} - 1\right]$$

$$n^{\varphi(m)} \equiv 1 \pmod{m} \Rightarrow m \mid \left[n^{\varphi(m)} - 1\right]$$

بما أن n, m أوليان فإن حاصل $n.m$ يقسم حاصل ضرب الحدين

$$n.m \mid (m^{\varphi(n)} - 1)(n^{\varphi(m)} - 1)$$

$$n.m \mid \left[\underbrace{m^{\varphi(n)} n^{\varphi(m)}}_{a} - \underbrace{m^{\varphi(n)} - n^{\varphi(n)} + 1}_{b}\right]$$

وأيضا نلاحظ أن $\underbrace{\quad}_{c}$ فإن

$$n.m \mid n^{\varphi(m)} . m^{\varphi(n)}$$

ويكون لدينا $n.m \mid [a]$ و $n.m \mid c$ فإن

$n.m \mid b$ وبالتالي فإنه يقسم الفرق بين

أي $n.m \mid \left[n^{\varphi(m)} + n^{\varphi(n)} - 1\right]$

$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{n.m}$$

$n \geq 2$

البرهان: اثبت أن $\varphi(n)$ هو عدد زوجي مهما كانت n عددا صحيحا.

(1) نفرض أن n تكتب على شكل عوامل أولية

أي الصيغة القانونية $n = p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

وحسب $\varphi(n)$

$$\varphi(n) = p_1^{\alpha_1-1} . p_2^{\alpha_2-1} \ldots p_k^{\alpha_k-1} (p_1-1)(p_2-1)\ldots$$

زوجي

$\frac{n}{p_1 . p_2 \ldots p_k} \prod (p_i-1)$ ناتجة من ضرب الحد

صحيح لأن p_i أولية فردية

التلاميذ 2 ... وبالتالي سيكون العدد زوجي

ب) إذا كان من الشكل $n = 2^k \; ; \; k \geq 2$

$$\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}(2-1) = 2^{k-1}$$

زوجي

ج) إذا كان ليس من الشكل السابق أي n لم يكن قوة للعدد 2 فيقبل القسمة على عدد فردي أولي وليكن p أي

$$n = p^s . m \; ; \; s \geq 1$$

ومن حيث $d(p,m)=1 \Leftarrow d(p^s, m)=1$ ومنه φ دالة ضربية يكون

$$\varphi(n) = \varphi(m) . \varphi(p^s)$$

$$= \varphi(m) . p^{s-1} (p-1)$$

زوجي

بنفس التفكير

عن المقدار $\varphi(n) = \varphi(m) . p^{s-1}$ ... يكون زوجية

تمرين: اثبت أن العدد (22) يقسم $22 / 3^{10n+2} + 5^{10n+1} - 2$

الحل:

$22 = 2.11$ $\quad (3^{10})^n . 3^2$

ونلاحظ

02

$d(3,22)=1$

$\Downarrow$

$3^{\varphi(22)} \equiv 1 \pmod{22}$ حسب أويلر نستطيع أن

$5^{\varphi(22)} \equiv 1 \pmod{22}$ $\Leftarrow$ $d(5,22)=1$

$\varphi(22) = 2 \cdot 11 = \varphi(2) \cdot \varphi(11) = 1 \cdot 10 = 10$

$3^{10} \equiv 1 \pmod{22}$ $\quad$ $5^{10} \equiv 1 \pmod{22}$

$\left[3^{10n+2} + 5^{10n+3} - 2\right] = \left[(3^{10})^n \cdot 3^2 + (5^{10})^n \cdot 5^3 - 2\right]$

نعوض التطابقات

$\equiv \left((1)^n \cdot 3^2 + (1)^n \cdot 5^3 - 2\right) \pmod{22}$

$\equiv (132) \pmod{22}$

22 mod تطابق الصفر $\quad$ $132 \div 22 = 6$, $132 - 132 = 00$

وبالتالي فإن

22 تقسم العدد

$\equiv 0 \pmod{22}$

مبرهنة: اثبت أن العدد n أولي إذا وفقط إذا كان $\varphi(n) = n-1$

إذا كان n أولي فإن $\varphi(n) = n-1$ لأن جميع الأعداد أصغر من n أولية مع n ($n-1$)

نفرض العكس أن $\varphi(n) = n-1$ ولنثبت أن n أولي.

لو كان n غير أولي لكان n مؤلف لوجد قاسم ليكن d

$1<d<n$; $d \mid n$ أي يوجد بين مجموعة الأعداد

$1, 2, 3, \ldots, n-1$ عدد واحد على الأقل

ليس أولي مع n وعندئذ سوف تكون $\varphi(n) \leq n-2$ وهذا

تناقض مع فرضنا $\varphi(n) = n-1$ ولذلك n لا يمكن أن يكون غير أولي

أي n أولي.

تمرين: لنفرض أن n عدد صحيح موجب ثم $\varphi(n)$ عندئذ

ملاحظة [illegible] 1- إذا كان n فردي فإن $\varphi(2n) = \varphi(n)$

2- n زوجي فإن $\varphi(2n) = 2\varphi(n)$

الحل: إذا كان n فردي فإن $d(2,n) = 1 \Rightarrow \varphi(2.n) =$

① $\varphi(2.n) = \varphi(2).\varphi(n) = 1.\varphi(n) = \varphi(n)$

② n زوجي : $n = 2^k.m \; ; \; d(2^k, m) = 1$

$\varphi(n) = \varphi(2^k.m) = \varphi(2^k).\varphi(m) = 2^{k-1}(2-1)$

$\varphi(m) = 2^{k-1}\varphi(m) \Rightarrow \varphi(2.n) =$

$\varphi(2.2^{k+1}.m) = \varphi(2^{k+1}.m)$

$\varphi(2^{k+1}).\varphi(m) = 2^k(2-1).\varphi(m)$

$\varphi(2n) = 2^k\varphi(m)$

$= 2.2^{k-1}.\varphi(m)$

$= 2.\varphi(n)$

تمرين: إذا كانت d جميع القواسم الموجبة لـ n فإن $\frac{n}{d}$ الدوال

يمسح $\frac{n}{d}$ جميع هذه القواسم. $n = 15$

الحل: إذا كان $d|n$ فإن $n = d.d_1$ $\quad d \in \{1, 3, 5, 15\}$

$d_1 = \frac{n}{d}$ حيث أن $\frac{n}{d} \in \{15, 5, 3, 1\}$ $\quad = 1+2+4+8 = 15$

$\varphi(1)+\varphi(3)+\varphi(5)+\varphi(15)$

$1+2+4+\varphi(3).\varphi(5)$

وبالتالي إذا أخذت d جميع قواسم n فإن $\frac{n}{d}$ تأخذ أيضاً جميع القواسم ومن ثم $\sum_{d/n} \varphi(d)$ تساوي

$$\sum_{d/n} \varphi(d) = \sum_{\frac{n}{d}/n} \varphi\left(\frac{n}{d}\right)$$

$n = 12$

n المعطى $d \in \{1, 2, 3, 4, 6, 12\}$

ما يقابلها هي

$\frac{n}{d} \in \{12, 6, 4, 3, 2, 1\}$

مبرهنة: $1 \leq n$ عدد صحيح فإن

$$n = \sum_{d/n} \varphi(d) = \sum_{d/n} \varphi\left(\frac{n}{d}\right)$$

مجموع قواسم العدد في دالة أويلر d/n تساوي دوماً العدد n.

الإثبات: نوزع الأعداد من $1, 2, 3, 4, \ldots, n$

في صفوف على النحو الآتي إذا كان

d/n : $S_d = \{m : d(m,n) = d\}$, $1 \leq m \leq n$

$S_3 = \{\ \}$

أي أن S_d تتألف ببساطة من الأعداد m

التي هي أصغر أو تساوي m وأكبر وتساوي 1

والقاسم المشترك مع هذه الأعداد يساوي d

أي أن عددها $\frac{\varphi(n)}{d}$

ولكن إذا كان $d(m,n) = d$ هذا يعني أن

$n = n_0 \cdot d$

$m = m_0 \cdot d$

حيث أن $d(n_0, m_0) = 1$ يوجد n_0, m_0

مثال:

$1, 2, 3, 4, 5, 6, \ldots$

$\ldots, 12, 13, 14, 15$

$S_3 = \{3, 6, 9, 12\}$

$S_5 = \{5, 10\}$

$S_{15} = \{15\}$

ويقابل كل عنصر m عنصر واحد m_0 لـ d واحد لـ d لذا

فإن عدد عناصر كل مجموعة S_d تساوي عدد الأعداد m_0

أي $\frac{m}{d} = m_0$ والأولية بالتسامح مع n_0 وهي $\frac{n}{d}$ والتي لا تتجاوز

n_0 أي أن عدد عناصر S_d يساوي عدد الأعداد الصحيحة

التي لا تتجاوز $\frac{n}{d}$ والأولية معها أي أن عدد S_d يساوي

$\varphi(\frac{n}{d})$ أي أن n

وبما أن كل من الأعداد في هذه المجموعة يقع في مجموعة

واحدة فقط من S_d نجد أن $n = \sum_{d/n} \varphi(\frac{n}{d})$ وهو نفسه $\sum_{d/n} \varphi(d)$

مثال: $n = 10$ قواسم n هي $\{1, 2, 5, 10\}$ ولنشكل المجموعات S_d

$S_1 = \{m ;\ d(m,10) = 1 ;\ 1 \le m \le 10\}$

$m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

$S_1 = \{1, 3, 7, 9\}$ الأولية مع S_1

$d(m,10) = 2$

$S_2 = \{2, 4, 6, 8\}$

$d(m,10) = 5$

$S_5 = \{5\}$ $\quad S_{10} = \{10\}$

- $|S_1| = 4 \Rightarrow \varphi(\frac{n}{d}) = \varphi(\frac{10}{1}) = \varphi(10) = 4$
- $|S_2| = 4 \Rightarrow \varphi(\frac{10}{2}) = \varphi(5) = 4$
- $|S_5| = 1 \Rightarrow \varphi(\frac{10}{5}) = \varphi(2) = 1$
- $|S_{10}| = 2 \Rightarrow \varphi(\frac{10}{10}) = \varphi(1) = 1$

ويصبح

$\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) =$
$1 + 1 + 4 + 4 = 10$

الدالات τ

تعريف الدالة (τ تاو): هي دالة حسابية فيمثلها عند العدد n بأنها عدد القواسم الموجبة المختلفة للعدد n

مثال: $\tau(3) = 2$ $\tau(4) = 3$ $\tau(5) = 2$ قواسم 5 {1,5}

قواسم 4 هي {1,2,4}

قواسم 10 هي {1,2,5,10} $\tau(10) = 4$

p أولي $\tau(p) = 2$

قواسم العدد p هي $1, p$.

برهان الدالة τ هي دالة ضربية

ملاحظة: يمكن استبدال الدالة τ

$\tau(n) = \sum (1)$

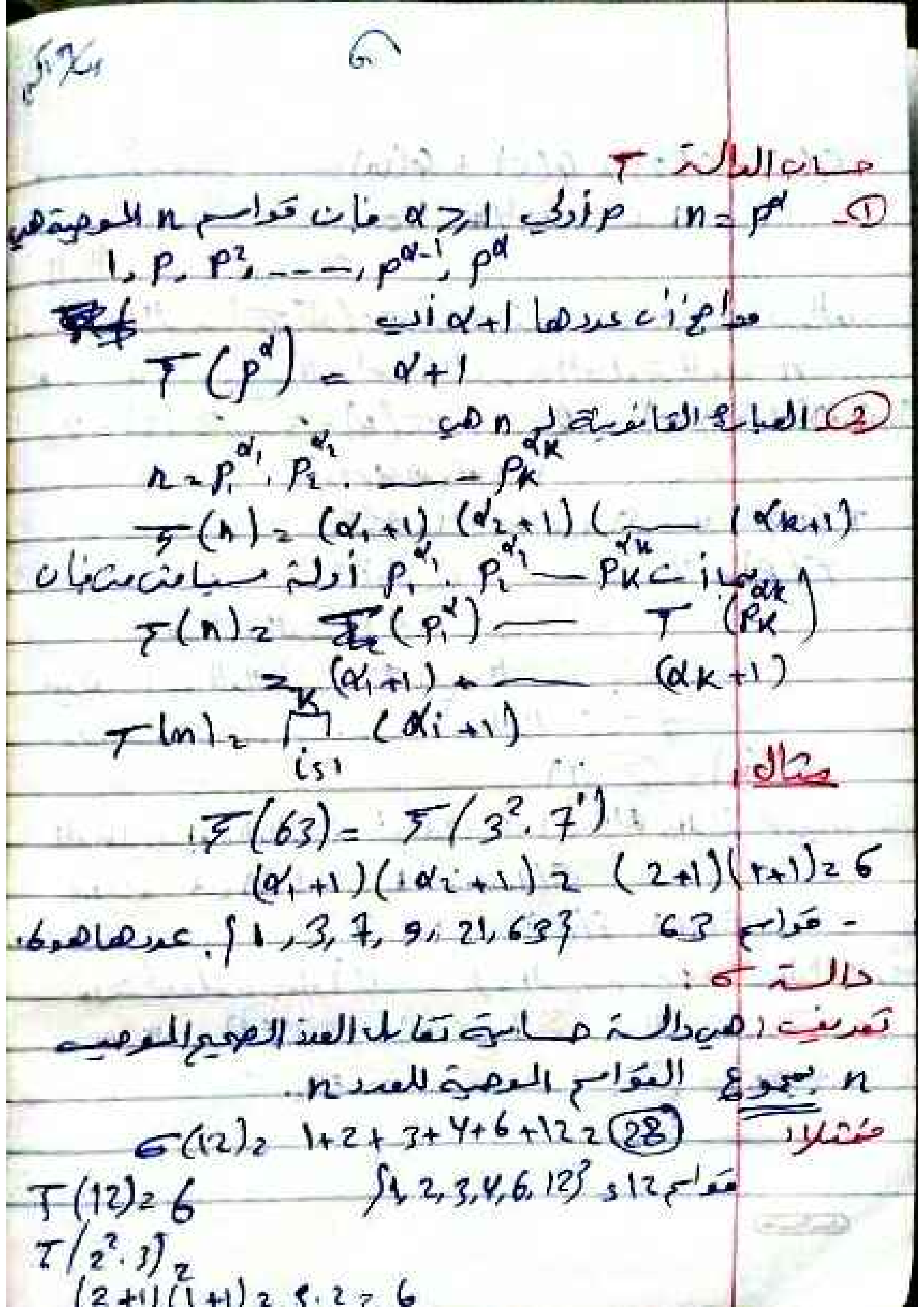
البرهان: إن الدالة $f(d) = 1$ لكل $d|n$ دالة ضربية تماماً

لأن $f(1) = 1$ $f(d_1 \cdot d_2) = 1$

$f(d_1) \cdot f(d_2) = 1 \cdot 1 = 1$

ولكن نعلم بأنه إذا كانت f دالة ضربية فإن الدالة المعرفة على النحو $F(n) = \sum f(d)$ ستكون دالة ضربية أيضاً.

ومنه تكون الدالة $\tau(n) = \sum_{d|n} 1$ $d|n$



دالة الثالثة τ:

① - لو $n = p^\alpha$ حيث p عدد أولي و $\alpha \geq 1$ فإن قواسم n الموجبة هي

$1, p, p^2, \dots, p^{\alpha-1}, p^\alpha$

وعددها $\alpha+1$ أي

$\tau(p^\alpha) = \alpha+1$

② الصيغة القانونية لـ n هي

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

$\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$

بما أن $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$ أولية فيما بينها مثنى مثنى

$\tau(n) = \tau(p_1^{\alpha_1}) \cdots \tau(p_k^{\alpha_k})$

$= (\alpha_1+1) \cdots (\alpha_k+1)$

$\tau(n) = \prod_{i=1}^{k} (\alpha_i+1)$

مثال:

$\tau(63) = \tau(3^2 \cdot 7^1)$

$(\alpha_1+1)(\alpha_2+1) = (2+1)(1+1) = 6$

- قواسم 63 {1, 3, 7, 9, 21, 63} عددها هو 6.

دالة σ:

تعريف: هي دالة حسابية تقابل العدد الصحيح الموجب n بمجموع القواسم الموجبة للعدد n.

مثلا:

$\sigma(12) = 1+2+3+4+6+12 = 28$

قواسم 12 هي {1, 2, 3, 4, 6, 12}

$\tau(12) = 6$

$\tau(2^2 \cdot 3) =$

$(2+1)(1+1) = 3 \cdot 2 = 6$

$\sigma(1)=1 \qquad \sigma(2)=3 \qquad \sigma(3)=4$

$\sigma(4)=1+2+3+4=7$

$$\boxed{\sigma(p)=1+p \qquad \tau(p)=2}$$

ويكتب بالشكل $\sigma(n)=\sum_{d/n} d = \sum_{d/n} f(d) \; ; \; f(d)=d$

بصورة سهلة بيان أن σ دالة ضربية

لأن الدالة المعرفة بالعلاقة $f(d)=d$ هي ضربية

تماماً: لأن $f(1)=1$ ، $f(d_1.d_2)=d_1.d_2=f(d_1).f(d_2)$

والدالة المعرفة بالشكل التالي $\sum_{d/n} f(d)$ ضربية

حساب الدالة σ :

① $n=p^\alpha$ إن قواسم $n=p^\alpha$ هي $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$

$\sigma(n)=1+p+p^2+\ldots+p^{\alpha-1}+p^\alpha$

هي مجموع متسلسلة هندسية حدها الأول يساوي (1) وأساسها p وعدد حدودها $\alpha+1$ ومنه يكون مجموعها

$$\boxed{\sigma(n)=\frac{1-p^{\alpha+1}}{1-p}}$$

[illegible] ①

② العبارة القانونية لـ n ، $n=p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}$ ، $\forall i, \alpha_i \geq 0$

$$\sigma(n)=\prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}$$

ملخص الدرس نظرية الأعداد

تتمة ما صنع نظرية الأعداد.

الانباح $p_k^{\alpha_k}$ ـــ $p_1^{\alpha_1}$ أولية قبلين منن

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \ldots \sigma(p_k^{\alpha_k})$$

$$= \frac{p^{\alpha_i+1}-1}{p_i-1} \cdot p_2$$

اذا كان p عدد أولي

$$\sigma(p) = \frac{p^2-1}{p-1} = \frac{(p-1)(p+1)}{p-1} = \boxed{p+1}$$

مثال: اوجد $\sigma(180)$ $\tau(180)$

180	2
90	2
45	3
15	3
5	5
1	

$$180 = 2^2 \cdot 3^2 \cdot 5$$

$$\sigma(180) = \sigma(\underset{p_1}{2^2} \cdot \underset{p_2}{3^2} \cdot \underset{p_3}{5})$$

$$\frac{2^3-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1}$$

$$= 7 \cdot 13 \cdot 6 = 546$$

$$\tau(180) = \tau(2^2 \cdot 3^2 \cdot 5)$$

$$(\alpha_1+1)(\alpha_2+1)(\alpha_3+1) = (2+1)(3+1)(1+1)$$

$$= 18$$

ملاحظة: ان الدالتين σ ، τ ليستا ضربية تماما.

حيث مثلا

$$\tau(20) = \tau(2 \cdot 10)$$ غير أوليين

$$\tau(2) \cdot \tau(10)$$ من خاصة آ ة ن

$$2 \cdot 4 = 8$$

$\tau(20) = (2^2 \cdot 5) = 6$

$\tau(2^2 \cdot 5) \neq \tau(2 \cdot 10)$ نلاحظ أن

فهي ليست ضربية تماما

$\sigma(20) = \sigma(2^2 \cdot 5) = \frac{2^3 - 1}{1} \cdot \frac{5^2 - 1}{5 - 1} = 7 \cdot 6 = 42$

$\sigma(2) \cdot \sigma(10) = 3 \cdot (1 + 2 + 5 + 10)$

$3 \cdot 18 = 54$

$\sigma(2^2 \cdot 5) \neq \sigma(2)\,\sigma(10)$

وبالتالي ليست ضربية تماما.

تمرين: اثبت أن جداء قواسم الموجبة للعدد n يساوي

$\prod d = (n)^{\frac{\tau(n)}{2}} = \sqrt{n^{\tau(n)}}$

الإثبات: $d/n \Leftarrow d'/n$

$n = d \cdot d'$

ولما كان عدد القواسم الموجبة لـ n يساوي $\tau(n)$

ومن ثم يكون لدينا عدد من العلاقات من $n = d \cdot d'$ تساوي $\tau(n)$

ونضرب هذه العلاقات نجد أن

$(n)^{\tau(n)} = \prod_{d/n} d \prod_{d'/n} d'$

وإذا مسحت d جميع قواسم n فإن

$d' = \frac{n}{d}$ تمسح جميع قواسم n أيضا

$\prod_{d/n} d = \prod_{d'/n} d'$

نوضح: $n = 10$

1 2 5 10

$10 = 1 \cdot 10$

$= 2 \cdot 5$

$= 10 \cdot 1$

$= 5 \cdot 2$

وبالتالي فان $(n)^{\tau(n)} = (\prod_{d/n} d)^2$ ومنه

$\prod_{d/n} d = \sqrt{n^{\tau(n)}}$

تمرين ٢ اثبت ان $\frac{\sigma(n)}{n} = \sum_{d/n} \frac{1}{d}$

او $\sigma(n) = n. \sum_{d/n} \frac{1}{d}$

الاثبات: نلاحظ بالتعريف ان $\sigma(n) = \sum_{d/n} d = \sum \frac{n}{d}$

ولتكن جميع قواسم n الموجبة هي

$d_1, d_2, \ldots, d_k$ فنجد

$$\sigma(n) = \frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k}$$

$$= n.\left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots \frac{1}{d_k}\right)$$

$$\sigma(n) = n \sum_{d/n} \frac{1}{d}$$

تمرين سؤال امتحان: أوجد العدد الصحيح n الذي يحقق العلاقة التالية

$\tau(10n) = 10$

الحل: $10 = 2.5$ هو جداء عددين أوليين لذا فان $10n$ يلزم ان يكون من الشكل

$10.n = 2^{\alpha} + 5^{\beta}$

وعندما يكون $\tau(10n) = (\alpha+1)(\beta+1) = 10 = 2 \cdot 5$

ومنه نجد ان: إما

$\alpha+1 = 2$, $\beta+1 = 5 \Rightarrow \alpha = 1$, $\beta = 4$

$\Rightarrow 10n = 2^1 \cdot 5^4 \Rightarrow n = 5^3 = 125$

أو:

$\alpha+1 = 5 \Rightarrow \alpha = 4$

$\beta+1 = 2 \Rightarrow \beta = 1$

$10n = 2^4 \cdot 5^1 \Rightarrow n = 8$

تعريف: نقول عن العدد الصحيح انه كامل أو تام اذا كان

$$\sigma(n) = 2n$$

أصغر عددين تامين كاملين معروفين $n = 6$, $n = 28$

$\sigma(6) = 12 = 2 \cdot 6$

- يقال عن العدد متوفر كامل اذا كان $\sigma(n)$ أكبر من $2n$
- يقال ان العددين m, n متحابان اذا كان

$\sigma(m) = \sigma(n) = m + n$

- ان العددين 220 , 284 عددان متحابان

ملاحظة: وجد العلماء عدد من الأعداد الكاملة وكلها زوجية وحتى الآن تبقى المسألة مفتوحة لوجود عدد كامل فردي.

- نسمي الأعداد من الشكل $M_k = 2^k - 1$ ، $k \geq 2$ أعداد ميرسين ونبحث عن الأعداد الأولية ذات الشكل M_k

أولية ميرسينية

تعريف دالة موبياس:

n عدد صحيح موجب بالشكل التالي:

$$\mu(n) = \begin{cases} 1 & ; \quad n = 1 \\ 0 & ; \quad p^2 / n \quad \text{p عدد اولي} \\ (-1)^r & ; \quad n = p_1 \cdot p_2 \cdots p_r \end{cases}$$

مثال:

$$\mu(30) = 2 \cdot 3 \cdot 5$$
$$= (-1)^3 = -1$$

$$\mu(10) = \mu(2 \cdot 5) = (-1)^2$$

$$\mu(12) = \mu(2^2 \cdot 3) = 0$$

ويرهن أن $\mu(n)$ دالة ضربية بشكل كامل

دالة ليوفيل: تعرف على النحو التالي

$$\lambda(n) = \begin{cases} 1 & ; \quad n = 1 \\ (-1)^{\alpha_1 + \alpha_2 + \cdots + \alpha_r} & ; \quad n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \end{cases}$$

البحث الأخير: الجذور الأولية والأدلة

المرتبة: إن رتبة a المقاس m أو الأس الذي ينسب إلى a بالمقاس m) حيث أن $d(a,m)=1$ هو اصغر عدد صحيح موجب k لا يساوي الصفر بحيث أن

$$a^k \equiv 1 \pmod m$$

ويقال عندئذ أن k هو دليل أو أن (دليل للعدد a بالمقاس m a) ويكتب $k = \operatorname{Ind}/a$

$= \operatorname{Ind} a \pmod m$

مثال: ماهي مرتبة 2 بالمقاس 7

$2^2 \equiv 4 \pmod 7$

$2^3 \equiv 1 \pmod 7$

أي مرتبة 2 بالمقاس 7 هي 3

$\operatorname{ord}_7 2 = 3$

$\operatorname{ord}_6 5 = 2 \qquad 5^2 = 1 \pmod 6$

$\operatorname{ord}_{14} 3 =$

$3^2 = 9 \pmod{14}$

$3^3 = 13 \pmod{14}$ 14|81

$3^4 = 11 \pmod{14}$

$\vdots$

$= 1 \pmod{14}$

بينما $3^6 \equiv 1 \pmod{14}$

$ord_{14} 3 = 6$

مبرهنة: اذا كان رتبة العدد الصحيح a بالنسبة للمقياس m تساوي K فإن $a^s \equiv 1 \pmod m$ إذا وفقط إذا $K | S$

البرهان: اذا كان K/S فإن $S = K.K_1$ ومن ثم

$a^s = (a^k)^{k_1} \equiv (1)^{k_1} \pmod m \equiv 1 \pmod m$

اذا كان S عدد صحيح يحقق $a^s \equiv 1 \pmod m$ حيث من خوارزمية القسمة

$s = q.k + r \quad 0 \le r < k$

$a^s = (a^k)^q . a^r \equiv 1 \pmod m$ و

$a^r \equiv 1 \pmod m$

ومن تعريف الرتبة لأن K هو أصغر عدد صحيح موجب يحقق الشرط يجب أن يكون $r = 0 \Leftarrow S = q.K \Leftarrow K | S$.

نتيجة: اذا كان K مرتبة a بالمقياس m فإن $K / \varphi(m)$

نفرض من مبرهنة أويلر $a^{\varphi(m)}$ يطابق العدد واحد بالمقياس m اذا كان $(a,m) = 1$ $a^{\varphi(m)} \equiv 1 \pmod m$

ومن المبرهنة السابقة فإن $K / \varphi(m)$

من هذه النتيجة نجد أن رتبة a بالمقياس m يجب أن تكون قاسم من قواسم $\varphi(m)$ حيث $\varphi(m)$ هو عدد الأعداد الأولية نسبياً مع m

مثال: اذا أردنا أن نجد $ord_{13} 2$

$ord_{13} 2$

اولاً نوجد $\varphi(13) = 12$

نوجد قواسم 12 وهي $\{1, 2, 3, 4, 6, 12\}$

فقط نوجد مع عدديته للعدد 2

$2^2 \equiv 4 \pmod{13}$

$2^3 \equiv 8 \pmod{13}$

$2^4 \equiv 3 \pmod{13}$

$2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 2^2 \pmod{13}$

$\equiv 12 \pmod{13}$

نعوض بين قبلها بالقاسم

$2^{12} \equiv 1 \pmod{13} \Rightarrow ord_{13} 2 = \varphi(13)$

فيقال أن العدد 2 له جذر أولي (أصلي) للعدد 13

وبشكل عام

- نقول أن العدد a له جذر أولي بالقياس m اذا وفقط اذا كان

$$ord_m a = \varphi(m)$$

مبرهنة: اذا كانت $ord_m a = k$ فإن

سؤال امتحان

$a^t \equiv a^s \pmod{m}$

اذا وفقط اذا $t \equiv s \pmod{k}$

البرهان: نفرض ان $a^t \equiv a^s \pmod{m}$ ونفرض ان $t \geq s$
وبما ان $d(a,m)=1$ فيمكن الاختصار على a^s ويكون
$$a^{t-s} \equiv 1 \pmod{m}$$
من المبرهنة الاولى $k \mid (t-s) \Leftarrow t \equiv s \pmod{k}$
$\Leftarrow$ من جهة ثانية نفرض ان $t \equiv s \pmod{k}$
نفرض ان $t \geq s$ من خوارزمية القسمة
$t = kq + s$
ومنه $a^t = (a^k)^q \cdot a^s$
$\equiv (1)^q \cdot a^s \pmod{m} \equiv a^s \pmod{m}$

ملاحظة: اذا كان $ord_m a$ is k فان الاعداد $\{a, a^2, \ldots, a^{k-1}, a^k\}$
تكون غير متطابقة بالمقياس m
- اذا كانت $ord_m a = k$ فان $ord_m a^r = \frac{ord_m}{d(k,s)}$

مبرهنة: اذا وجد جذر اولي للعدد m وكان هذا الجذر هو a
$d(a,m)=1$ اي $ord_m a = \varphi(m)$ فان للعدد m يوجد
$\varphi(\varphi(m))$ جذراً اولياً.
- اذا كان p عدد اولي و r جذر اولي للعدد p اي ان
$ord\, r = p-1$
فان عدد الجذور الاولية لـ p هو $\varphi(p-1)$

مثال: $p=7$ فان $\varphi(7)=6$ عدا $\varphi(6)$
$\varphi(6)=2$ $1, 2, 3, 6$
ومنه للعدد 7 هنالك جذران اوليان هما $3, 5$